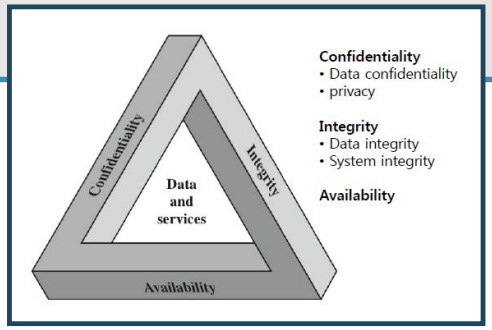
GS224-3

أمن المعلومات

عناصر أمن المعلومات

الاهداف

- التعريف بعناصر أمن المعلومات و ماهيتها .
- تحديد عناصر أمن المعلومات و أمثلة لكل منها .
- توضيح دور عناصر أمن المعلومات و تأثير غيابها .
- إبراز دور التكامل بين عناصر أمن المعلومات لتوفير الحماية اللازمة للمعلومات .



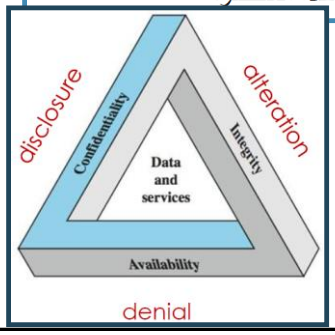
عناصر أمن المعلومات

وسواءً أكانت المعلومة مستقّرة في قواعد بيانـات أو وسائط تخزين ثابتة، أم يتم تبادلها بين طرفين، فإنه لا بد من وجود القناعة التامة بتحقيق حد معين من أمن المعلومات في حال استقرارها أو نقلها. ويتحقّق هذا الحدّ من خلال عناصر أمن المعلومات، التي هي عبارة عن عدة عناصر كلّ واحد منها يغطي جانبًا مهمًا من جوانب أمن المعلومات، وإذا كان هناك خلل أو غياب لأحد هذه العناصر، فإنّه سيكون هناك قصور في أمن المعلومة من ذلك الجانب.

لقـد حـدّد بعضـ المؤلّفـين ثـلاث ركائـز أساسيـة لأمـن المعلومـات هـي: السِّريّـة (Confidentiality)، وسلامـة المعلومـة وتكاملهـا (Integrity)، والتوفر (Availability)، وأُطلق على ذلك مثلث (CIA) (CIA Triangle) . إلّا أنّ الاتحاد العالمي للاتصالات في توصيته X.800[1] قد حدّد عناصر أساسية لأمن المعلومات يمكن حصرها في سبعة عناصر رئيسة، هي: التحقّق من الهُويّة، والتحكم بالوصول، والسرية، وسلامة المعلومة وتكاملها، وعدم الإنكار، وتوافر أو ديمومة المعلومة، والمتابعة أو التدقيق .

عناصر أمن المعلومات

يمكن تعريف عناصر أمن المعلومات بأنّهـا: «مجموعة العناصر الواجب توافرها لحماية المعلومات الثابتة والمنقولة، بحيث يغطّي كلّ عنصر من هذه العناصر جانبًا من جوانب الحماية المطلوبة. ومعنى ذلك هو أن تتكامل هذه العناصر حتى توفّر الحماية المطلوبة، وفي حال فقد أيّ منها فسيكون هنالك خلل أمنيٌّ في الجانب الذي يغطّيه هذا العنصر.



1- التحقق من الهوية (Authentication)

تعني الخدمة التي يمكن من خلالها التحقّق من هُويّة الشخص(أو الجهة) وأنّه الشخص المعني لا غيره. فعند اتصال شخصين(أو جهتين) بعضهما ببعض، فلا بدّ من أن يتعرّف كل منهما إلى الآخر، لضمان أن يتخاطب كلّ منهما مع الشخص أو الجهة المعنيّة وليس مع غيرها. بعبارة أخرى: فإنّ التحقّق من الهُويّة هو التحقّق مـن أنّ المستخدم لنظام ما هو بالفعل من ادّعى أنّه ذلك المستخدم[1]، وفي حال نقل المعلومات، فإنّه يجب التحقّق من هُويّة المرسل لضمان أنّ المعلومة قادمة من مصدرها الحقيقي، وكذلك يجب التحقّق من هُويّة المستلم لضمان أنّ المعلومة ذاهبة إلى وجهتها الصحيحة.

تبدأ عملية التحقّق مـن الهُويّة بالتعريف بالهوية أو تحديـد الهُويّة(Identification). ويمكن تحقيق ذلك من خلال اسم المستخدم أو رقم الحساب مثلًا. إنّ تحديد هوية الشخص أو التعريف به رقميًّا(إلكترونيًّا) أمر مهم، وقد يكون صعبًا في بعض الأحيان؛ إذ إنّ الشخص الواحد نفسه قد يكون لديه أكثر من هوية رقميّة.

1- التحقق من الهوية (Authentication)

- **معايير طرق تحديد الهوية :**
  - ان تكون الهوية فريدة بمعنى ان تكون غير قابلة للتكرار.
  - أن تكون غير مفصحة عن معلومات المستخدم و وظيفته و الغرض من الوصوله الى المعلومة.
  - أن لا تكون مشتركة بين المستخدمين.
  - أتباع معايير المعتمدة عند المؤسسة عند أنشاء حسابات ألمستخدمين.
- **عناصر التحقق من الهوية :**
  - التحقق من هوية الشخص أو الجهة : التحقق من هوية طرفى الاتصال فى جميع مراحله و عدم قدرة المعتدى على انتحال شخصية أحد الطرفين.
  - التحقق من أصل منشأ المعلومة : التحقق من أصل المعلومة بأنها صادرة من جهتها الأصلية – تأكيد مصدر المعلومات – بمعنى ارسلت من الجهة التى تدعى انها ارسلتها.

1- التحقق من الهوية (Authentication)

- التحقّق باستخدام معيار واحد: هذا المعيار هو «**ماذا تعرف؟**» كاستخدام كلمات المرور أو أرقام التعريف الشخصية (Personal Identification Number-PIN). ويعتمد هذا المعيار في التحقّق من الهُويّة على طلب (إدخال) معلومة **لا يعرفها** إلا الشخص المعني فقط، ويُعدُّ من أدنى درجات التحقّق من الهُويّة.
- التحقّق باستخدام معيارين: ويتم ذلك باستخدام معيار «**ماذا تعرف؟**»، بالإضافة إلى معيار آخر هو «**ماذا تملك؟**» وتعتمد هذه الطريقة في التحقّق من الهُويّة على طلب (إدخال) معلومة **لا يعرفها** إلا الشخص المعني فقط، ومعلومة أخرى **لا يملكها** إلا الشخص نفسه أيضًا.
- التحقّق باستخدام ثلاثة معايير: ويتم ذلك باستخدام معيار «**ماذا تعرف؟**» ومعيار «**ماذا تملك؟**» بالإضافة إلى معيار ثالث هو «**من أنت؟**». وتعتمد هذه الطريقة في التحقّق من الهُويّة على طلب (إدخال) معلومة **لا يعرفها** إلا الشخص المعني فقط، ومعلومة أخرى **لا يملكها** إلا الشخص نفسه، ومعلومة ثالثة من واحدة أو أكثر من **خصائص الشخص** الحيويّة التي تميّزه من غيره، كبصمات الأصابع والعين، وأبعاد راحة اليد والوجه، والتعرّف إلى الصوت، وغير ذلك. وتوفّر هذا الطريقة أعلى درجات التحقّق من الهُويّة، لكنها تحتاج إلى أجهزة وبرامج إضافيّة، وتُعدُّ أكثر تعقيدًا من سابقاتها.

2- التحكم في الوصول (Access Control)

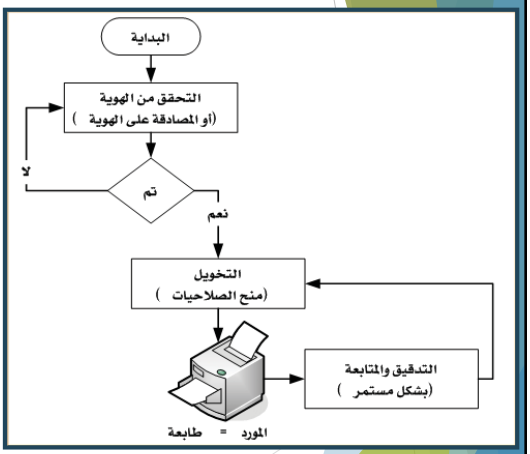
التحكّم بالوصول هو طُرُق (أو وظائف) الحماية التي تتحكّم بوصول المستخدمين أو الأنظمة إلى موارد المنشأة، كالأجهزة الرئيسة والبيانات المركزيّة، أو بعبارة أخرى: منع الاستخدام غير المرخص به للموارد . فتلك الطُّرُق هي التي تحمي الأنظمة وموارد المنشأة المختلفة من الوصول غير الشرعي، كما أنها تساعد في تحديد مستوى التّخويل (Authorization) المصرّح به بعد نجاح عملية التحقّق من الهُويّة.

- **مراحل التحكم بالوصول**: لكى يتمكن مستفيد ما - مستخدم أو برنامج أو عملية ما أو غيره – من الوصول الى مورد ما و استخدامه أو الاستفادة منه فإنه يجب ان يمر برمحلتين أوليتين للتحكم بوصوله الى ذلك المورد هما : التحقق من الهوية و التخويل ثم مرحلة ثالثة بعد وصوله للمورد و استخدامه وهى التدقيق و المراقبة ، وكما هو موضح فى الشكل التالى .

2- التحكم في الوصول (Access Control)

مراحل التحكم بالوصول

1. **التحقق من الهوية** : هو الطريقة للتأكد من أن المستفيد هو من أدعى انه هو، وبشكل عام ، تلزم التحقق من المستفيد كخطوة أولى للوصول الى موارد المؤسسة.
2. **التخويل أو الترخيص** : وهى التاكد من أن المستفيد الذى جرى التعرف عليه و المصادقة علي هويته لديه الصلاحيات و الامتيازات التى تخوله استخدام المورد وتنفيذ العمليات التى يريدها عليه.



2- التحكم في الوصول (Access Control)

2. **التخويل او الترخيص :** معايير التحكم فى منح الصلاحيات و مراجعتها دوريا
   - المنح بناء على دور المستخدم و مهامه فى المؤسسة و العمل الذى يقوم به.
   - المنح بناء على الموقع الذى به المستخدم نسبة الى المورد.
   - المنح فى أوقات محددة للتعامل و التواصل فى اوقات و تواريخ مع المورد.
   - المنح بناء على الاجراء (العملية) المزمع اجراءها على البيانات و المورد المستخدم.
   - منح الصلاحيات للمجموعات اذا احتاجوا لنفس الصلاحيات على بيانات و موارد معينة .
   - عدم السماح الافتراضى او التلقائي (البدء من صفر صلاحيات ثم الاضافة حسب الحاجة)
3. **التدقيق و المتابعة :** متابعة عملية المستخدمين على الموارد و تسجيلها من أجل مراجعتها و معرفة اى خلل او تجاوز فى الصلاحيات الممنوحة لكل مستخدم و اتخاذ الاجراءات المناسبة بناء على النتائج :
   - حجب المستخدم نهائيا أو تعطيل حسابه وبذلك لا يمكنه استخدام اى مورد نهائيا
   - حجب المورد عن جميع المستخدمين بمن فيهم من صدر منه التجاوز
   - حجب صلاحيات معينة من المستخدم الذى صدر منه التجاوز

3- السرية (Confidentiality)

يمكن أن يطلق على هذا العنصر أيضًا الخصوصيّة(Privacy) وتعني الحفاظ على المعلومات من أن يطّلع عليها(يقرأها ويفهمها) غير الأشخاص المصرّح لهم فقط، أو بعبارة أخرى: منع الكشف غير المصرّح به[1] . فعندما تُرسل رسالة «سريّة»، فإنّ ذلك يتطلّب أن لا يراها إلا المرسِل والمرسَل إليه فقط. فإنّ استطاع أحد الاطّلاع عليها، فإنّه لا يستطيع أن يفهم محتواها، أي يجب أن تكون غير مفهومة له.

هناك العديد من الطرق لتوفير السِّريّة تتراوح بين حجب المعلومة يدويًّا، وعدم تسليمها إلّا للأشخاص المصرّح لهم فقط إلى طُرُق التشفير الحديثة التي تعتمد على خوارزميّات رياضيّة معقّدة يصعب فكّها، إن لم يكن مستحيلًا. من هنا يمكن القول إنّه يمكن توفير عنصر السِّريّة من خلال تشفير البيانات سواءً الثابتة منها أو المنقولة، وتطبيق سياسة صارمة للتحكّم بالوصول، وتصنيف المعلومات، وتدريب العاملين على أنظمة وسياسات أمن المعلومات تدريبًا جيّدًا.

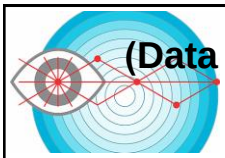
3- السرية (Confidentiality)

قد يستطيع المهاجمون إحباط فاعليّة عنصر السِّريّة، باستخدام عدّة طُرُق من أهمّها: مراقبة الشبكة، وهجوم تصفّح الكتف، والهندسة الاجتماعيّة. قد يكشف المستخدم عن بعض المعلومات الحسّاسة عمدًا، أو عن طريق الخطأ عندما لا يقوم بتشفير هذه المعلومات، أو عندما يقع ضحيّة لهجمات الهندسة الاجتماعيّة، أو بسبب اللامبالاة والإهمال وغياب الحسّ الأمني عند معالجة مثل هذه المعلومات.

من الأمثلة المشهورة على هذه الخروقات أيضًا، حفظ ملفات النّسخ الاحتياطي في مكان خارج المنشأة، لكنّها غير مشفّرة(وهو في حدّ ذاته إجراء سليم؛ لأنّه لا بدّ من حفظ بعض هذه النُّسخ في مكان بعيد عن المنشأة، حتى يمكن الرجوع إليها في حال تدمير المنشأة بالكامل، لكن لا بدّ من تشفيرها، إذا لم يقم نظام النسخ الاحتياطي بذلك) . في هذه الحالة أُخرِجت معلومات المنشأة من داخل منظومة أمن معلوماتها نهائيًّا مهما كانت قوتها و وضعت خارجها. فإذا لم تكن مشفّرة فهي عرضة للاطّلاع عليها وفهمها من قبل الآخرين.

أمثلة: السرية

- **معلومات عن معدلات/درجات الطلبة** تعتبر بيانات سرية بمستوى عالي ، حيث ان بعض القوانين تحدد عرضها للطالب أو ولى أمره أو المستخدمين عندما تتطلب العلاقة المهنية ذلك.
- **معلومات عن تسجيل الطلبة** ربما تعتبر بمستوى سرية متوسط ، حيث الضرر محدود لو كشفت.
- **معلومات عن دليل الهاتف** بمستوى منخفض حيث هي مكشوفة للجميع



4- سلامة المعلومة و نزهتها (Data Integrity)

تعني الخدمة التي من خلالها يمكن الحفاظ على سلامة المعلومة من التعديل، أو الحذف، أو الإضافة، أو إعادة التركيب، أو إعادة التوجيه. وهذا أمر مهمّ جدًّا لضمان الثقة في المعلومة وأنّها هي المعلومة الأصلية دون زيادة أو نقصان. فقد تكون المعلومة مشفّرة وسرّيّتها مضمونة، لكن قد تتعرّض للتغيير طالما أنّها معلومة إلكترونيّة. هذا التغيير لا بدّ من إيجاد طريقة لكشفه، وهو ما يوفّره هذا العنصر، وقد يترتّب على ذلك إلغاء المعلومة وعدم الاعتماد عليها بالكليّة.

تعني سلامة المعلومة وتكاملها بأنّه تم تلقّي الرسالة تمامًا كما أرسلت بالفعل. وهذا الأمر يولّد الثقة لدى المتعامل مع المعلومة من أنّها كاملة في محتواها لم تنقص شيئًا، وأنّها صحيحة في مضمونها لم يطرأ عليها أيّ تغيير، وأنّه جرت معالجتها أثناء تنقّلها (كالحفظ وإعادة الإرسال) بالطرق الصحيحة التي لم تُحدث فيها أيّ تغيير متعّمد أو غير متعّمد.

4- سلامة المعلومة و نزهتها (Data Integrity)

يهتم هذا العنصر بعمليّة "كشف" عدم سلامة المعلومة وتكاملها أكثر من اهتمامه بعمليّة "منع" التعديل على المعلومة، أو "تصحيح" ذلك التعديل. والسبب في ذلك، أن أي تعديل غير مشروع على المعلومة، يجعلها معلومة غير آمنة حتى وإن جرى تصحيح التعديل. فما الفائدة من ذلك التصحيح إذا كانت المعلومة قد وصل إليها آخر وعرفها، وربما احتفظ بنسخة منها لديه؟ وهنا تبرز أهميّة كشف إعادة توجيه الرسالة وكشف إعادة تركيبها، لأنّه في مثل هذه الأحوال تصل الرسالة كاملة لكنّها غير سليمة، ولا تقف قدرة الكشف عند كشف التعديل الذي ينتج عنه تشويه واضح في المعلومة، بل يتعدى الأمر ذلك إلى كشف أيّ تعديل، حتى لو بقيت المعلومة بعده كأنها لم تتغيّر، ومثال ذلك أن يجري تغيير التاريخ أو الوقت أو اليوم إلى تاريخ أو وقت أو يوم آخرين يبدو لمتلقّي المعلومة معه أنّ شيئًا لم يتغيّر، بينما الواقع غير ذلك. فمثلًا

أمثلة : النزاهة

- **معلومات عن حساسية مريض بمستشفى ذات مستوى نزاهة عالي** : الطبيب يثق بأن المعلومات صحيحة و حديثة ، فمثلا لو ممرضة زورت البيانات تعمدا ، يجب ان تكون هناك إمكانية لقاعدة البيانات لاسترجاع البيانات لأصلها و تتبع البيانات لمعرفة من قام بالتزوير .
- **بيانات التسجيل في مجموعة او منتدى على الشبكة المعلوماتية يعتبر بمستوى نزاهة متوسط.**
- **الاستبانة المجهولة/العامة على الشبكة المعلوماتية تعتبر ذات مستوى نزاهة منخفض** (عدم الصحة امر طبيعي).

5- عدم الانكار – التنصل (Non -Repudiation)

هي الخدمة التي من خلالها يمكن منع أيّ شخص أو جهة من إنكار أيّ عمليّة قاموا بها وكشفهم. فعلى سبيل المثال إذا منحت جهة معيّنة الصلاحية لجهة أخرى لشراء منتج معيّن، ثم أنكرت بعد ذلك أنّها منحت هذه الصلاحية لتلك الجهة، فإنّ خدمة عدم الإنكار ستكشف ذلك.

في حالة إرسال رسالة بين طرفين، فإنّ عدم الإنكار يثبت إرسال المرسل لها ويثبت استقبال المستقبل لها، بحيث لا يمكن لأيّ منهما إنكار ذلك، وتزداد أهميّة هذا الإثبات بازدياد أهميّة الرسالة نفسها.

تشمل خدمة عدم الإنكار أيضًا إثبات وقوع العمليّات والإجراءات الإلكترونيّة في أوقات وتواريخ معيّنة عن طريق إلحاق بصمة التاريخ والوقت بالعمليّة نفسها (Time Stamping).

6- توفر المعلومة / الخدمة (Availability)

يقصد بتوافر المعلومة، أن تكون قابلة للوصول إليها واستخدامها حين الطلب من قبل أيّ شخص أو أيّ جهة معروفة ومحدّدة وفي أيّ وقت (مصرّح به)[1]. ويمكن القول إنّ خدمة التوافر هي الخدمة التي تحمي النظام ليبقى متاحًا دائمًا (ومن هنا يطلق عليها أحيانًا «الديمومة») وهي موجّهة خصيصًا إلى أيّ خلل أو هجوم يمكن أن يؤدّي إلى عدم توافر الخدمات، ومن أمثلة ذلك: هجوم الفيروسات، وهجمات حجب الخدمة أو منعها (Denial of Service-DoS). ويتطلّب هذا الأمر في غالب الأحيان حماية ماديّة تقنيّة كتقنيات توفير نظم احتياطية للمعلومات والطاقة الكهربائيّة.

6- توفر المعلومة / الخدمة (Availability)

إنّ الهدف العام من عنصر توافر المعلومة هو أن تكون الشبكة والأجهزة والأنظمة والبرامج والخدمات متاحة في جميع الأوقات التي يحتاج إليها المستخدم، وأن توفّر لها الحماية مما قد يتسبب في عطل أو عدم توفر أي منها، وفي حال حدوث الأعطال أو الكوارث المعلوماتيّة يجب أن تكون هناك شبكة وأجهزة وأنظمة وبرامج بديلة يجري إحلالها آليًّا وبسرعة فائقة محلّ تلك التي تعرّضت للعطل أو الكارثة، وفق خطّة تشغيل للطوارئ يتم إقرارها والتدريب عليها جيّدًا قبل ذلك.

تجدر الإشارة إلى أنّه لا بدّ من الموازنة بين الحماية وتوافر المعلومات. فإذا سُمح لأيّ شخص بالدخول إلى المعلومة في أيّ وقت ومن أيّ مكان وبأيّ طريقة اتصال؛ فإنّنا بذلك نحصل على درجة عالية من توافر المعلومة، لكن في المقابل ينتج عن ذلك ثغرات أمنيّة كبيرة وكثيرة جدّاً، وبالمقابل، فإنّه إذا جرى تقييد المعلومات بشكل كبير من أجل حمايتها فسيكون من الصعب توفير المعلومات لجميع الشرائح التي تحتاج إليها في الاوقات المناسبة، والمطلوب هو الموازنة بين ذلك؛ للوصول إلى منزلة وسطية بين المنزلتين.

أمثلة : التوافر

- **نظام يقدم خدمة المصادقة:** مطلوب مستوى توفر عالي ، فمثلا اذا لم يتمكن مستخدم من التواصل مع مورد ما ، قد يؤدى هذا لخسائر مالية
- **موقع عام على الشبكة المعلوماتية لجامعة:** هذا يتطلب مستوى توفر متوسط حيث انه غير حساس و لكن عدم توفر الخدمة امر يسبب الاحراج.
- **دليل هاتف على الشبكة المعلوماتية:** ذو مستوى توفر منخفض حيث عدم توفر الخدمة يسبب مضايقة (يمكن إيجاد حلول أخرى).

7- المتابعة والتدقيق (Auditing)

تهدف المتابعة(ويطلق عليها أحيانًا المحاسبة(Accountability)) إلى متابعة عمليّات المستخدمين والتحقق من فرض سياسات أمــن المعلومات، وأنّها تطبّق بشكل صحيح ودقيق. كما يمكن استخدام نتائج المتابعة كأدوات تحقيق(Investigation Tools) في حالة خرق أنظمة أمن المعلومات لإثبات وقوع بعض الأحداث، وإثبات إدانة المستخدم(أو المتهم) أو براءته من القيام بذلك الحدث.

7- المتابعة والتدقيق (Auditing)

- **اسباب ضرورة اجراء المتابعة و التدقيق :**

1. للتحقق من أن الاجهزة والانظمة والبرامج تعمل بشكل طبيعى وذلك من مراجعة سجلات الاحداث (Log File)، والتى تمكننا من الاجراء المناسب، مثل:
   - معرفة الاخطأ (Errors) التى تقع ، حيث سيوجد فى السجل رسالة خطأ توضح تفاصيله
   - معرفة رسائل التحذير(Alerts) التى تنبئ عن إمكانية حدوث مشكلة ما.
   - توفير المعلومات (Information) عن الاحداث التى تتم لمجرد الاخبار عنها و اخذ العلم بها فقط.
2. لمراقبة العمليات السيئة التى قد يقوم بها المستخدمين (عمدا او سهوا) .
3. للكشف عن عمليات التطفل و الاختراق
4. للمساعدة على استعادة الاحداث و معرفة متطلبات الاجهزة و اعداداتها ، لأستعادتها كما كانت عند حدوث مشكلة.
5. تشكل مصدر قانونيا رسميا للمؤسسة لاثبات الاحداث أو نفيها .
6. تشكل مصدر من المصادر التقارير الرسمية للمؤسسة عن انشطتها و المشاكل التى قد تقع فيها أو في أنظمتها.

7- المتابعة والتدقيق (Auditing)

عند إجراء عمليّات التدقيق والمتابعة يجب مراعاة النقاط الآتية:

- حفظ وثائق المتابعة كسجلّات الأحداث في مكان آمن.
- استخدام أدوات المتابعة المناسبة يؤدي إلى نتائج أفضل بحجم أقل من المعلومات، حيث إن من أكبر المشكلات التي تواجه أنظمة المتابعة هي كبر حجم معلومات المتابعة التي يلزم مراجعتها، وقد يكون بعضها غير ضروري.
- يجب المحافظة على معلومات المتابعة وسجلّات الأحداث من التغيير غير الشرعي حتى لا تفقد مصداقيتها وقانونيتها.
- يجب تدريب العاملين في حقل المتابعة، ومراجعة وثائق المتابعة جيّدًا؛ للحصول على أفضل النتائج وبأسرع الأوقات.
- حصر صلاحيّة حذف وثائق المتابعة وسجلّات الأعمال في مديري الأنظمة(Administrators) الموثوق بهم فقط.
- لا بدّ أن تشمل المتابعة جميع الأحداث، بما في ذلك الأحداث الخاصة بذوي الصلاحيّات العليا، مثل مديري الأنظمة.

7- المتابعة والتدقيق (Auditing)

- **الاحداث التى تشملها المتابعة و التدقيق :**

1. **الاحداث على مستوى الانظمة** (كأنظمة التشغيل و الخوادم)، وتشمل: أداء النظام ، محاولات الدخول للنظام، عمليات تعطيل حسابات المستخدمين، عمليات تفعيل حسابات المستخدمين، استخدام ادوات ادارة النظام، استخدام موارد النظام، العمليات الاساسية، طلبات تغيير اعدادات النظام.
2. **الاحداث على مستوى البرامج التطبيقية**، وتشمل: رسائل الخطأ و المستخدمين الذين ظهرت لهم، الملفات التى تفتح و تغلق، التغييرات التى تحدث على الملفات، مخالفات أمن المعلومات و السياسات الامنية التى ترتكب داخل البرنامج.
3. **الاحداث على مستوى المستخدمين**، وتشمل: محاولات تحديد الهوية و التعريف بها و المصادقة عليها (سواء كانت ناجحة او فاشلة)، الملفات و الخدمات والموارد التى يستخدمها، الاوامر التى انشأها، مخالفات أمن المعلومات و السياسات الامنية التى ارتكبها أو تسبب بها.

مستويات تأثير الاختراق الامني

- **منخفض:** الفاقد له تأثير محدود، بمعنى تراجع في الخدمة ، ضرر بسيط ، خسارة مالية غير مهمة أو أذى طفيف.
- **متوسط:** الفاقد له خطير ، بمعنى تراجع مهم خدمة ، أذى جدي للأشخاص ولكن بدون فقدان للحياة أو تهديد بإصابات.
- **عالي:** الفاقد له تأثير شديد أو كارثي غير مرغوب به على الخدمة ، أصول المؤسسة (موارد النظام) ، على الأشخاص (فقدان للحياة).

المتطلبات الوظيفية/العملية للأمن

- **الإجراءات التقنية**
  - التحكم في الوصول ؛ التعرف و المصادقة ؛ حماية النظام و الاتصالات ؛ نزاهة المعلومات و النظام
- **الإجراءات الإدارية**
  - التدريب و التوعية ؛ التفتيش و المحاسبة ؛ الترخيص ؛ الاعتماد و التقييم الأمني ؛ التخطيط للطوارئ ؛ الصيانة ؛ حماية بيئة العمل ؛ التخطيط ؛ الامن الشخصي ؛ تقييم المخاطر.
- **تداخل و تشابك الإجراءات التقنية مع الإدارية**
  - تهيئة الإدارة ؛ الاستجابة للحوادث ؛ حماية الوسائط.

مبادئ التصميم الأساسية للأمن [1/2]

لايزال من الصعب تصميم نظام يمنع العيوب الأمنية بشكل كامل و لكن تم توثيق ممارسات جيدة يمكن الاستنارة بها لتصميم جيد يحد من العيوب الأمنية:

- **آلية اقتصادية :** تصميم التدابير الأمنية يجب ان يكون بسيطاً قدر الإمكان
  - سهل الإنجاز و التحقق
  - اقل عرضة للوهن
- **أساس الفشل الامن :** قرارات الوصول يجب ان تعتمد على التصاريح (الأصل منع الوصول).
- **التوسط/التدخل الكامل:** يجب مراجعة كل وصول حسب نظام التحكم في الوصول.
- **تصميم مفتوح:** التصميم يجب ان يكون مكشوف و ليس سري (مثل خوارزميات التشفير).
- **التغليف:** يخفي البنية الداخلية.
- **النمطية:** مبنى كوحدات تركيبية.

مبادئ التصميم الأساسية للأمن [2/2]

- **العزل:**
  - يجب عزل الوصول العام عن الموارد الحرجة (لا يوجد اتصال بين عامة المستخدمين و المعلومات الحرجة)
  - يجب عزل ملفات المستخدمين بعضها عن بعض (عدى عند الحاجة).
  - يجب عزل آليات الامن (منع الوصول لهذه الآليات).
- **الطبقية:** استخدام طرق و وسائل حماية متنوعة و متداخلة (الحماية العميقة) .
- **اقل دهشة:** يجب ان تكون استجابة البرنامج أو واجهة المستخدم بشكل اقل دهشة أو ذهول للمستخدم.
- **فصل الامتيازات:** الوصول الناجح للنظام يتطلب عدة امتيازات او تراخيص (او انجاز عمل ما).
- **اقل امتيازات:** كل مستخدم (عملية) يجب ان يملك اقل الامتيازات لأداء عمل ما.
- **ادنى أليات مشتركة:** يجب ان يقلل التصميم من الوظائف المشتركة ما بين المستخدمين المختلفين (توفير الامن المتبادل ؛ تقليل من الايصاد).
- **مقبول نفسيا:** يجب على آليات الامن ان لا تتعارض على نحو غير ملائم مع عمل المستخدمين.

مواضع الهجوم/الاختراق

- **مواضع الهجوم:** هو محل الضعف او الثغرة الذى يمكن الوصول اليه او يمكن استغلاله في النظام.
  - نقاط الربط المفتوحة
  - الخدمات التي خارج حماية جدار الامن
  - موظف له إمكانية الوصول لمعلومات حساسة
- **ثلاثة أصناف**
  - موضع الهجوم في الشبكات (مواضع الثغرات بالشبكة)
  - موضع الهجوم في البرمجيات (مواضع الثغرات بالبرنامج)
  - موضع الهجوم على المستخدمين (الهندسة الاجتماعية)
- **تحليل الهجوم:** تقييم حجم و خطورة التهديدات على النظام.

شجرة الهجوم/الاختراق

- تفرعات هيكلية لبنية بيانات تمثل مجموعة تقنيات محتملة يمكن ان تستغل نقاط الضعف او الوهن الامنية بالنظام.
- الحدث الأمني والذي هو هدف المهاجم يتم تمثيله في الشجرة كعقدة الأصل و الطرق المتابعة للوصول للهدف يتم تمثيلها تتابعيا كتفرعات و عقد جانبية في الشجرة.
- كل حلقة تفرعية تبين هدف جانبي ، وكل هدف جانبي ربما له اهداف فرعية تتبعه ، الخ. العقدة النهائية في المسار الخارج من عقدة الأصل (أوراق الشجرة) تمثل عدة طرق لتنفيذ هجوم أمني.
- كل عقدة عدى الأوراق هي عقدة-أو (احداها) او عقدة-و (جميعها) . للتحقيق الهدف الممثل بواسطة عقدة-و يجب تحقيق جميع الأهداف الفرعية الممثلة بالعقد المتفرعة منها، ولكن لتحقيق الهدف الممثل بواسطة عقدة-أو يكفى تحقيق هدف فرعي واحد على الأقل.
- يمكن تمييز التفرعات بقيم تمثل الصعوبة ، التكلفة ، أو خصائص أخرى للهجوم بحيث يمكن مقارنته بهجوم آخر.
- يمكن للمحلل الأمني من استخدام الشجرة لترشيد التصميم و تقوية الإجراءات المضادة.

شجرة الهجوم/الاختراق

الشكل التالي يوضح مثال لتحليل شجرة هجوم لتطبيق مصادقة حساب مصرفي على الانترنت. عقدة أصل الشجرة هي هدف المهاجم ، المربعات المظللة على الشجرة هي الأوراق والتي تمثل احداث تتضمن الهجوم، في حين ان المربعات الغير مظللة عبارة عن أنواع أخرى يمكن ان تحتوى على حدث هجوم معين او اكثر. لاحظ في الشجرة ان جميع العقد عدى الأوراق هي على شكل عقدة-أو (احداها).

التحليل المستخدم لبناء هذه الشجرة مبنى على المكونات المستخدمة في عملية المصادقة:

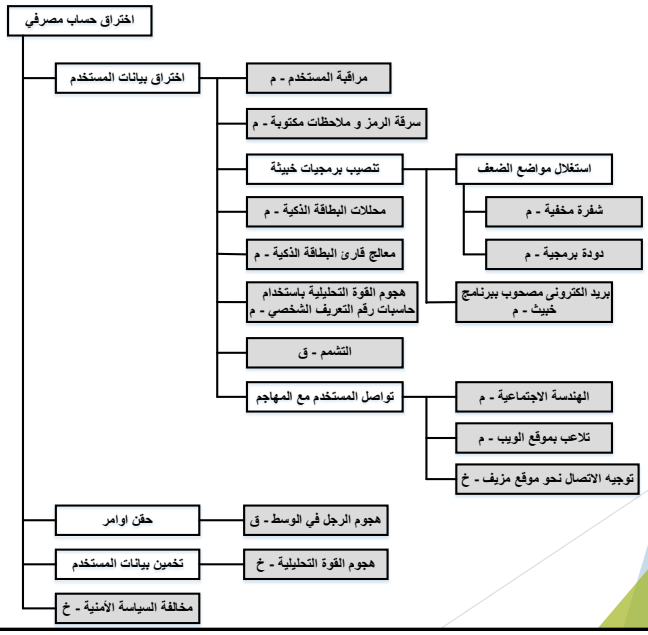
- **المستخدم و المحطة الطرفية للمستخدم (م)** : هذا الهجوم يستهدف معدات المستخدم ، البطاقات الذكية و كلمات المرور كذلك أفعال المستخدم.
- **قناة الاتصال (ق)** : هذا النوع من الهجوم يركز على روابط الاتصال.
- **خادم المصرف على الشبكة (خ)** : هذه الأنواع من الهجوم هي هجومات غير مباشرة ضد الخادم الذي يستضيف تطبيق المصادقة المصرفية.

أربعة أنواع من هجومات يمكن تحديدها، كل منها يستغل احدى او اكثر من المكونات السابقة ، هذه الأنواع من الهجمات هي:

شجرة الهجوم/الاختراق

- **اختراق بيانات المستخدم:** هذه الاستراتيجية يمكن استخدامها ضد مواضع هجوم عدة . توجد لها عدة إجراءات هجومية مثل مراقبة أفعال المستخدم بملاحظة ارقامه السرية او غيرها من بيانات المصادقة ، او سرقة البطاقة الذكية او ملاحظاته مكتوبة. الخصم يمكن ان يخترق او يكشف معلومات البطاقات باستخدام أدوات هجوم مختلفة، مثل اختراق البطاقات الذكية ، او استخدام أسلوب القوة التحليلية لتخمين الرقم السري. استراتيجية أخرى محتملة هي تضمين برمجية خبيثة لاختراق اسم و كلمة مرور المستخدم. يمكن للخصم ان يحاول الحصول على معلومات المصادقة عن طريق التنصت على قناة الاتصال (التشمم/الالتقاط). في النهاية، الخصم يمكن ان يستخدم عدة طرق لمشاركة الاتصال مع المستخدم المستهدف.
- **حقن أوامر:** في هذا النوع من الهجوم، المستخدم له القدرة على اعتراض الاتصال بين المحطة الطرفية للمستخدم و خادم المصرف على الشبكة. هناك عدة طرق مستخدمة تمكن من التنكر على شكل مستخدم شرعي و كسب إمكانية الوصول الى النظام المصرفي.
- **تخمين بيانات مصادقة المستخدم:** لوحظ ان هجومات القوة التحليلية ضد نظم المصادقة المصرفية ممكنة بأرسال اسم و كلمة مرور مستخدم عشوائية. و تعتمد علي آلية وجود حواسيب مجندة موازعة و هي تستضيف برمجيات لحساب اسم او كلمة مرور المستخدم.
- **مخالفة السياسات الأمنية:** مثال على ذلك ، مخالفة السياسات الأمنية للمصرف بربط آلية الدخول بتحكم ضعيف في الوصول، الموظف بذلك يسبب في حادث امنى داخلي قد يعرض حسابات الزبون للاختراق.

مثال : شجرة هجوم مختصرة لاختراق حساب مصرفي



استراتيجية أمن المعلومات

- **الاستراتيجية العامة لتوفير الامن**
- **الخطة:** ماذا يجب ان تدعم لنظم الامن
  - الأصول و قيمتها
  - سهولة الاستخدام ضد الامن
  - تكلفة الامن ضد تكلفة الفشل/الاصلاح
- **الإنجاز/الآلية:** كيفية فرض،
  - المنع
  - الاكتشاف
  - الاستجابة
  - الاصلاح
- **الصحة/الضمان:** هل مضمونة حقا (الفعالية/النقد/المراجعة).

وقعة الامن

من المستوى الأعلى، يحقق المهاجم أو مجموعة من المهاجمين غاياتهم من خلال تنفيذ الهجوم ، وقد تتكون الواقعة من هجوم واحد أو عدة هجمات (كما هو موضح في دورة الإعادة). العناصر الرئيسية لوقعة الهجوم هي:

- **الفعل** (Action): خطوة يتخذها المستخدم أو العملية من أجل تحقيق نتيجة .
- **الهدف** (Target): كيان معنوي او مادى بالحاسب الألى أو الشبكة.
- **حدث** (Event): فعل موجه إلى هدف ما بقصد أن يؤدي إلى تغيير حالة أو حالات الهدف.
- **الأداة** (Tool): وسيلة لاستغلال ضعف/ثغرة بنظام الحاسب أو الشبكة.
- **الثغرة** (Vulnerability): ضعف في النظام يسمح بفعل غير مصرح به.
- **العواقب** (Unauthorized result): نتائج غير مرغوبة لحدث ما.
- **الهجوم** (Attack): سلسلة من الخطوات يتخذها المهاجم لتحقيق نتائج غير مرغوبة.
- **المهاجم** (Attacker): الشخص الذي يحاول تنفيذ هجومًا واحدًا أو أكثر من أجل تحقيق غاية ما.
- **الغاية** (Objectives): الغرض أو الهدف النهائي للحادثة.
- **الواقعة** (Incident): مجموعة من الهجمات يمكن تمييزها عن بعضها البعض وذلك لتميز المهاجمين والاعتداءات والأهداف والمواقع والتوقيتات.

وقعة الامن